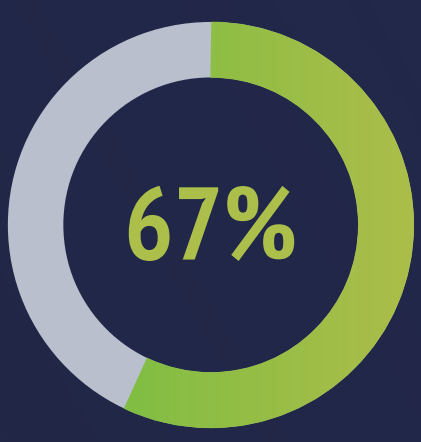
CHIME PUBLIC POLICY

WORKING FOR YOU IN WASHINGTON

IT REMAINS CLEAR THAT CONGRESS AND THE EXECUTIVE BRANCH MUST ACT TODAY TO HELP SECURE HEALTHCARE

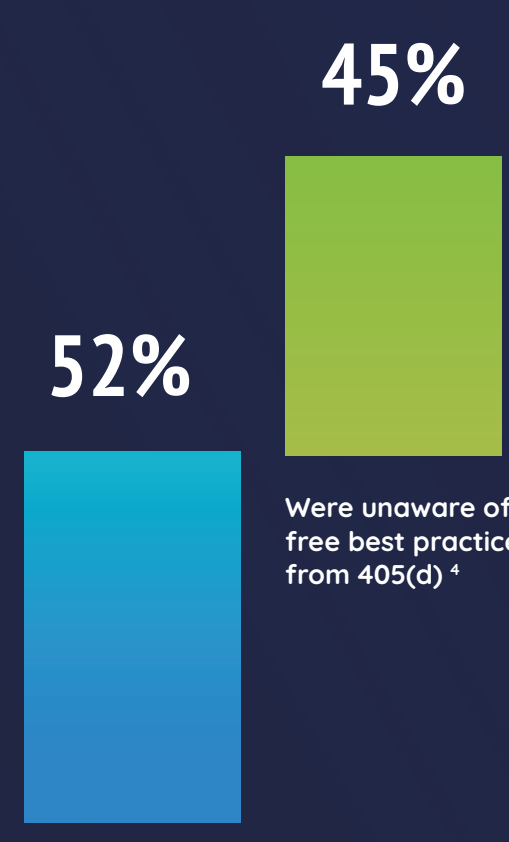
As part of its advocacy efforts surrounding cybersecurity CHIME and AEHIS polled its membership in a survey to better understand the threats their organizations face, the resources they need and the education gaps that currently exist. The results continue to outline what those who have been active in the cybersecurity landscape have known for years, **healthcare is under constant threat, more resources are needed for healthcare providers and significant education gaps remain.**



of respondents indicated they'd had a security incident in the last 12 months

MOST COMMON SECURITY EXPLOITS

- PHISHING/EMAIL COMPROMISE
- MALWARE
- RANSOMWARE
- HACKING
- INSIDER THREAT



Were unaware of free best practices from 405(d) [4]

Are members of an ISAC and ISAO[3]

EMERGING SECURITY THREATS[1]

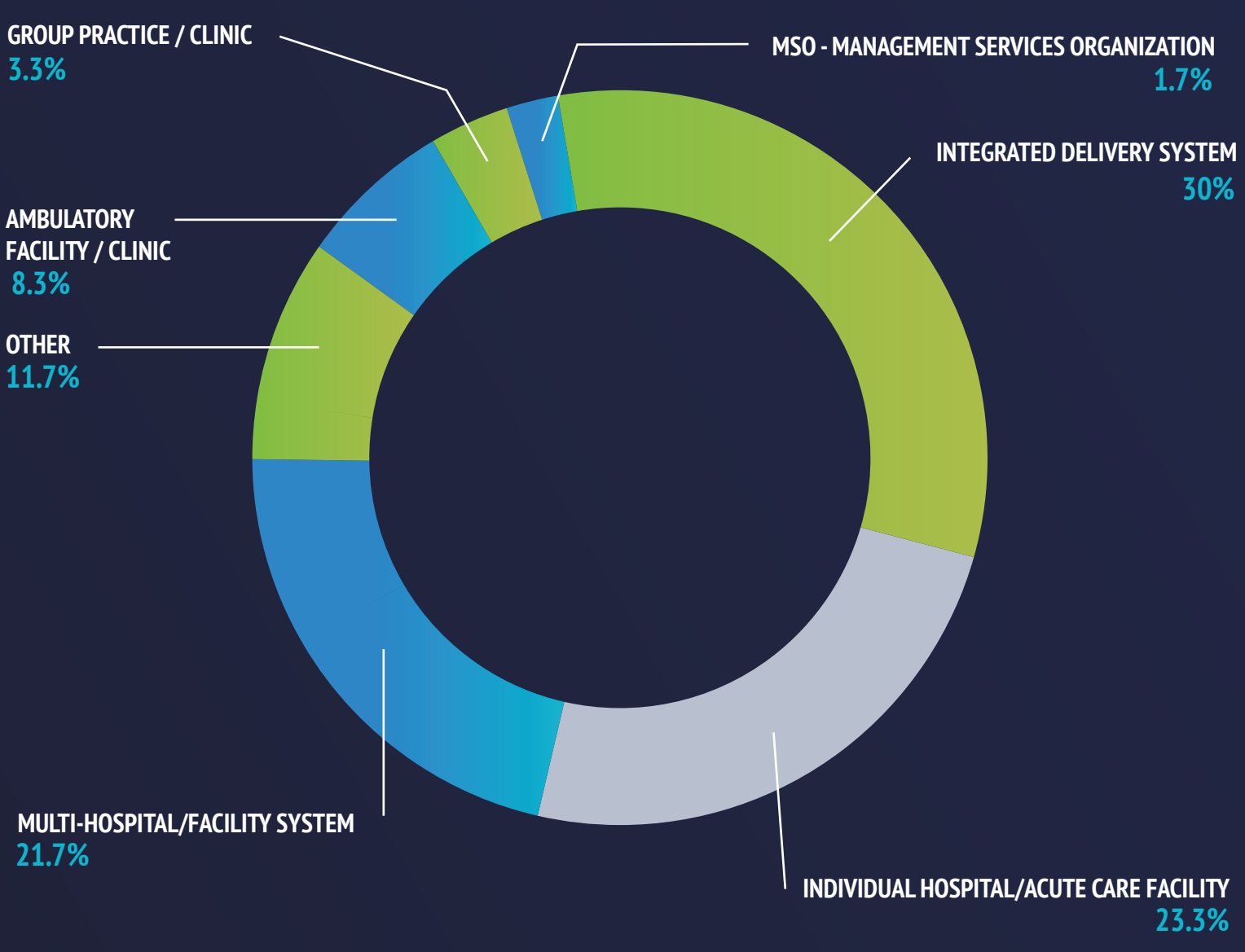
- IOT/CONNECTED DEVICES
- INCREASED REMOTE WORKFORCE
- SUPPLY CHAIN
- 3RD PARTY CONSUMER HEALTH APPS
- API[2] SECURITY

80%

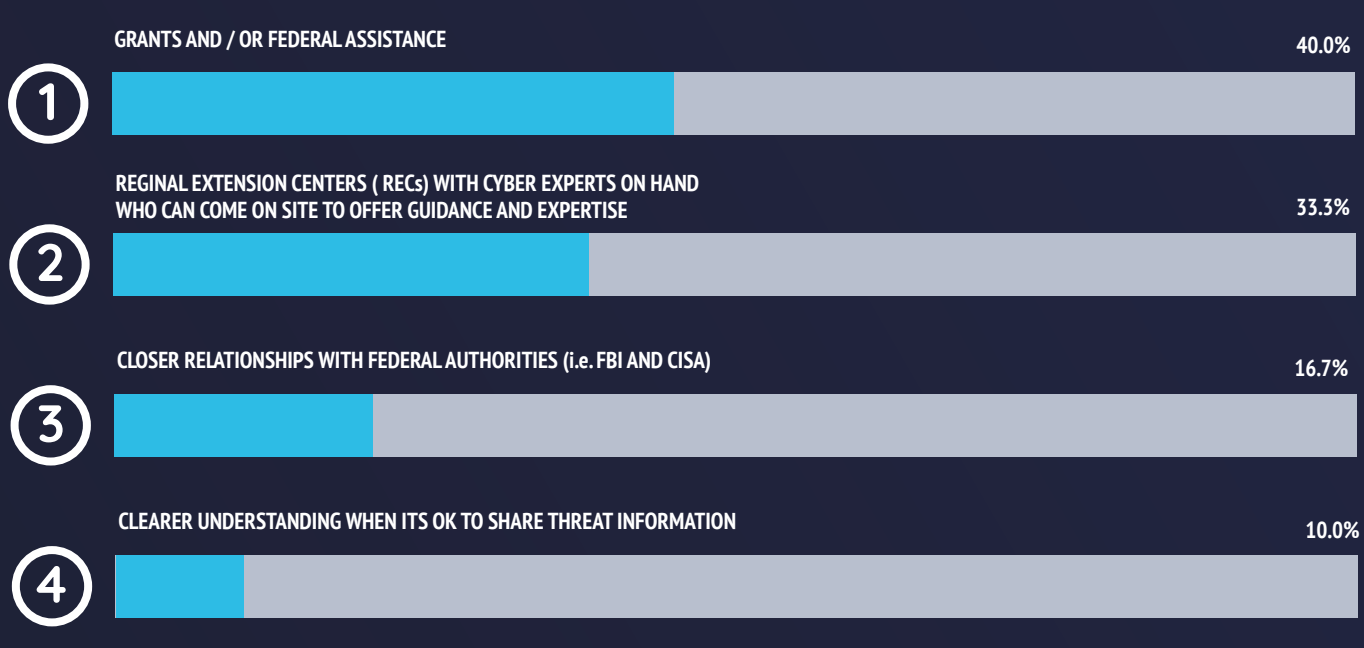
OVER 80% RESPONDENTS INDICATED THE COST OF CYBER INSURANCE HAD INCREASED OVER THE PAST YEAR

ALL TYPES OF ORGANIZATIONS ARE SUBJECT TO CYBERATTACKS

WHAT BESTS DESCRIBES YOUR ORGANIZATION TYPE?



PROVIDERS REPORT THEY NEED HELP IN VARIOUS AREAS



FOOTNOTES

1 - OVER THE NEXT THREE YEARS

2 - APPLICATION PROGRAMMING INTERFACES

3. INFORMATION SHARING & ANALYSIS CENTER (ISAC)
INFORMATION SHARING AND ANALYSIS ORGANIZATION (ISAO)

4. 405(D) BEST PRACTICES WERE DEVELOPED JOINTLY BETWEEN THE SECTOR AND THE U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES (HHS)

https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx

CHIME AEHIS